حملات سایبری چیست؟

حمله سایبری یک **اقدام مخرب** و **آگاهانه** توسط یک فرد یا سازمان برای نقض **سیستم اطلاعاتی شخص یا سازمان** دیگر است. معمولاً مهاجم به دنبال نوعی مزاحمت برای ایجاد اختلال در شبکه قربانی است.
حملات سایبری در لیست خطرات جهانی **رتبه پنجم** را در سال ۲۰۲۰ به خود اختصاص داده است و به یک قاعده جدید در بخش های دولتی و خصوصی تبدیل شده است. این صنعت پر خطر در سال ۲۰۲۱ همچنان در حال رشد است، زیرا انتظار می رود حملات سایبری اینترنت اشیا به تنهایی **تا سال ۲۰۲۵ دو برابر** شود.
جرایم اینترنتی که شامل سرقت یا اختلاس گرفته تا هک و تخریب داده ها می باشد، در نتیجه شیوع COVID-19 حدود ۶۰۰٪ افزایش یافته است.

حملات سایبری چند بار رخ می دهد؟

حملات سایبری هر روز به مشاغل آسیب می زند. این آسیب ها بعضی از مشاغل را از پای در می آورد و بعضی دیگر می توانند با تلاش به روال خود باز گردند.

دو نوع شرکت وجود دارند: شرکت هایی که هک شده اند، و کسانی که هنوز نمی دانند هک شده اند.

تأثیر و شدت حملات سایبری

حملات سایبری می تواند از بسیاری جهات بر سازمان ها تأثیر بگذارد، از اختلالات جزئی در عملیات گرفته تا خسارات عمده مالی. صرف نظر از نوع حمله سایبری، هر نتیجه ای نوعی هزینه دارد چه پولی و چه غیر پولی.

پیامد های حملات سایبری ممکن است هفته ها و یا ماه ها بعد بر روی کسب و کار شما تأثیر بگذارد. در ادامه پنج منطقه ای که ممکن است تجارت شما آسیب ببیند را لیست کرده ایم:

- خسارات مالی
- از دست دادن بهره وری
- خسارت به اعتبار شما
- مشکلات مداوم تجاری

چرا افراد حملات سایبری را انجام می دهند؟

از زمانی که افراد از سیستم های تجاری آسیب پذیر بهره مند می شوند، جرائم سایبری افزایش یافته است. غالباً مهاجمان به دنبال **باج گرفتن** هستند: ۵۳ درصد از حملات سایبر منجر به خسارت ۵۰۰,۰۰۰ دلاری یا بیشتر شده است.

اهداف حملات سایبری می تواند بسیار متنوع باشد: از سرقت اطلاعات گرفته تا ایجاد مانع برای عدم دسترسی به سرویس دهنده ها و صدها مورد دیگر...

بات نت چیست؟

بات نت شبکه ای از دستگاه های آلوده به نرم افزارهای مخرب مانند ویروس است. مهاجمان با هدف افزایش میزان حملات خود می توانند یک بات نت را به عنوان گروه کنترل کنند. غالباً از یک بات نت برای غلبه بر سیستم ها در یک حمله ی توزیع شده از انکار سرویس (DDoS) استفاده می شود.

انواع متداول حملات سایبری

حملات سایبری شامل انواع متداولی می باشد که در ادامه آن ها را بررسی می کنیم:

بد افزار

بد افزار اصطلاحی است که برای توصیف نرم افزارهای مخرب از جمله **نرم افزارهای جاسوسی**، باج افزارها، ویروس ها و کرم ها به کار می رود. بدافزارها از طریق آسیب پذیری یک **شبکه** را نقض می کنند.
به طور معمول هنگامی که کاربر روی پیوند خطرناک یا پیوست نامه ای از طریق ایمیل کلیک می کند و سپس نرم افزار مخاطره آمیز را نصب می کند. پس از داخل شدن به سیستم، بدافزار می تواند موارد زیر را انجام دهد:

- دسترسی به مؤلفه های اصلی شبکه را مسدود می کند.
- بدافزار یا نرم افزار مضر اضافی را نصب می کند.
- به طور پنهانی با انتقال داده ها از هارد اطلاعات را به دست می آورد.
- برخی از مؤلفه ها را مختل کرده و سیستم را غیرقابل اجرا می کند.

فیشینگ عملی است، که از طریق ارسال پیام های جعلی که به نظر می رسد از یک منبع معتبر می باشد، انجام می شود و معمولاً هم از طریق ایمیل اتفاق می افتد.
هدف از این کار **دزدی اطلاعات حساس** مانند کارت اعتباری و اطلاعات ورود به سیستم یا نصب نرم افزار های مخرب در دستگاه قربانی می باشد، فیشینگ یک شیوه رایج سایبری است.

دو نقطه ورود مشترک برای حملات:MitM

۱. در Wi-Fi نا امن عمومی، مهاجمان می توانند خود را بین دستگاه بازدید کننده و شبکه قرار دهند و بدون اطلاع، بازدید کننده تمام اطلاعات را از طریق مهاجم منتقل می کند.
۲. هنگامی که بدافزار به دستگاهی رخنه کرد، یک مهاجم می تواند نرم افزاری را برای پردازش تمام اطلاعات قربانی نصب کند.

تکذیب سرویس حمله

یک حمله تکذیب سرویس باعث می شود، سیستم ها، سرورها یا شبکه هایی را که دارای ترافیک برای خروج منابع و پهنای باند هستند، طغیان کنند. در نتیجه، سیستم قادر به انجام درخواست های مشروع نیست. مهاجمین همچنین می توانند از چندین دستگاه به خطر بیافتند تا این حمله را انجام دهند.

بهره برداری از حمله روز صفر یا(Zero – day)

پس از اعلام آسیب پذیری شبکه، یک بهره برداری صفر روز مشاهده می شود و در حقیقت پیش از آن که توسعه دهندگان بتوانند راه حلی برای آن بیابند، توسط مهاجمان استفاده شده و یا به اشتراک گذاشته می شود.

چگونه خطر حملات سایبری را کاهش دهیم؟

با افزایش تهدیدات هکر هایی که اطلاعات شما را نادرست کنترل می کنند، اجرای فرآیند های جلوگیری از نقض امنیت داده بعد از داشتن بیمه حرفه ای و کافی برای نقض داده، از بهترین اقدامات است.

قوانین نقض داده ها در هر کشور متفاوت است، بنابراین بسته به محل کار شما، عوامل مختلفی باید در نظر گرفته شوند. نوتیفیکیشن های مربوط به این نقض، مواردی که تحت پوشش قرار گرفته اند و مجازات ها بسته به بروز و وضعیتی که در آن قرار دارید متفاوت خواهد بود. اما:

۱- انتقال داده ها را کاهش دهید

انتقال داده ها بین دستگاه های شخصی و تجاری، اغلب به دلیل افزایش روز افزون کارمندانی که از راه دور کار می کنند، اجتناب ناپذیر است. نگهداری اطلاعات حساس در دستگاه های شخصی آسیب پذیری در برابر حملات سایبری را به میزان قابل توجهی افزایش می دهد.

۲. دانلود فایل ها

از منابع تأیید نشده می تواند سیستم ها و دستگاه های شما را در معرض خطرات امنیتی قرار دهد. برای کاهش حساسیت دستگاه خود در برابر بدافزار، مهم است که فقط فایل ها را از منابع معتبر دانلود کنید و از دانلود های غیر ضروری خودداری کنید.

۳. امنیت رمز عبور را بهبود ببخشید

قدرت رمز عبور اولین خط دفاعی در برابر حملات مختلف است. با استفاده از ترکیبی از نماد ها که معنی ندارند، تغییر رمز عبور به طور منظم و ذخیره نکردن آن یا به اشتراک گذاری آن، یک مرحله حیاتی برای محافظت از اطلاعات حساس شماست.

۴. سیستم عامل دستگاه خود را به روز کنید

ارائه دهندگان سیستم عامل دستگاه ها به سختی کار می کنند تا به طور مداوم سیستم عامل خود را ایمن تر کنند و نصب منظم آخرین به روزرسانی ها باعث آسیب پذیری کمتر دستگاه در برابر حملات می شود.

۵. نظارت بر نشت داده ها

نظارت منظم بر داده های شما و شناسایی نشت های موجود به کاهش تأثیر احتمالی نشت طولانی مدت داده ها کمک می کند. ابزار های نظارت بر نقض داده ها فعالیت مشکوک را به طور فعال کنترل کرده و به شما هشدار می دهند.

۶. پلن پاسخ به نقض داده را ایجاد کنید

نقض داده حتی برای دقیق ترین و با نظم ترین شرکت ها نیز ممکن است اتفاق بیفتد. ایجاد یک برنامه رسمی برای مدیریت حوادث احتمالی به سازمان ها در هر اندازه ای کمک می کند تا در برابر حملات واقعی پاسخ دهند و آسیب های احتمالی آن ها را مهار کنند.